METHOD AND APPARATUS FOR DETECTING PROTECTION OF AUDIO AND VIDEO SIGNALS

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to audio and/or video data and more particularly to copy protection of such audio and/or video data.

BACKGROUND OF THE INVENTION

Unauthorized copying of copyrighted works is, unfortunately, very prevalent in our society. Such unauthorized copying ranges from simple copying of a few pages from a copyrighted book to black market distribution of millions of dollars worth of illegally copied movies, compact discs, and other entertainment medium.

With the advent of DVD, the illegal copying of DVD's is of great concern to content companies (i.e., the companies owning the copyrighted work recorded on the DVDs). To protect the copyrighted works, content companies are demanding that DVD produces incorporate a security mechanism to prevent unauthorized copying. One such security mechanism is currently being used in conjunction with video cassette recorders and was developed by Macrovision.

The Macrovision anti-taping technique (herein after referred to as Macrovision) works due to the differences in the way VCRs and televisions operate. The automatic gain control (AGC) circuits within a television respond slowly to change, while a VCR's AGC respond quickly to change. Macrovision takes advantage of this difference by modifying the video signal so that a television will still play it properly, while a VCR will not record a viewable picture. Macrovision accomplishes this by utilizing at least one of Sync pulse adjustment, vertical blanking pulses, and end of field pulses. This technique is being contemplated as an adequate part of a solution for copy protection for DVDs.

While Macrovision prevents VCRs coupled to televisions from making quality copies, it does not prevent unauthorized copying when a VCR, or any other video source (including a DVD player), is coupled to a personal computers ("PC"). As is generally known, a PC may be equipped with an analog video decoder, such as the All-in-Wonder, manufactured by ATI Technologies, Inc., which converts an analog video signal into a digital video data stream, where the analog video stream originated from a video source, such as a DVD player. Such an analog to digital conversion strips out the Macrovision encoding. As such, a DVD player sourcing the analog video to the PC may have the copyrightable work copied without the Macrovision encoding. Such unauthorized copying is unacceptable to content companies.

Therefore, a need exists for a method and apparatus that detects the presence of encoded copy protection information embedded in a video data stream such that a PC cannot make quality copies of the video data.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a schematic block diagram of a circuit that detects embedded protection coding within an audio and/or video data stream, such a circuit is in accordance with the present invention;

FIG. 2 illustrates a graphical representation of a field of video data which is in accordance with the present invention;

FIG. 3 illustrates a typical horizontal video line which includes embedded protection coding in accordance with the present invention;

FIG. 4 illustrates a computer system that includes a embedded protection detecting circuit which is in accordance with the present invention;

FIG. 5 illustrates a logic diagram that may be used to detect embedded protection information in accordance with the present invention;

FIG. 6 illustrates a logic diagram that may be used to detect embedded copy protection coding in a video data stream in accordance with the present invention; and

FIG. 7 illustrates a logic diagram that may be used to detect embedded protection information in a data stream in accordance with the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Generally, the present invention provides a method and apparatus for protecting access to audio and/or video data. This may be accomplished when data is received, where the data may be audio data and/or video data. Having received the data, it is interpreted to determine whether an embedded data access parameter is active. If so, an indication of the particular type of data access is generated. The data access parameter may control access to the data as at least one of: copy restrictions, viewing restrictions, and/or use restrictions. The indication is subsequently provided to a computer system such that unauthorized accessing, including unauthorized copying, of the video and/or audio data is prohibited. With such a method and apparatus, a personal computer (PC) may be coupled to receive audio and/or video data from a data source, such as a DVD player, detect whether the data being sourced is protected, and, if so, ensure that the data is protected based on the data access parameter.

FIG. 1 illustrates a schematic block diagram of a computer system **10** that is equipped to detect the presence of embedded data access parameters in a data stream. The data stream may be representative of video data **18** or audio data which could be sourced by a television, VCR, DVD player, audio amplifier, etc. The computer system **10** is shown, in part, to include a central processing unit **12**, memory **14**, and a video decoder **16**. The central processing unit **12** may be any type of central processing unit incorporated into a personal computer, such as those manufactured by Compaq, IBM, etc., a video game player, or a set-top entertainment PC. The memory **14** may be read only memory, random access memory, or cache memory.

The video decoder **16** includes a graphics controller **20** and a video digitizer **22**. The video digitizer **22** receives the video data **18** and converts it into a digital video stream; as a by-product of the analog to digital conversion, the embedded protection coding that resides in the synchronization portions (i.e., horizontal and vertical sync) of the video data is lost. The resulting digital video data **26** is provided to the memory **14** for storage therein. As stored, the digital video data **26** does not include the embedded protection coding, such that, without the present invention, the digital video data **26** could be readily copied as directed by the central processing unit **12**.

The graphics controller **20**, however, prevents the central processing unit **12** from directing any such authorized access to the digital data by providing it with an indication of protection **24**. The graphics controller **20** generates the indication of protection **24** by monitoring the video data **18** for the embedded protection coding. When detected, the graphics controller **20** provides the indication of protection

to the central processing unit which is programmed to respond accordingly. The indication may be an indication that some form of protection is available (Eg. that the video data is encoded with Macrovision) or the indication may clearly define the particular type of protection. For example, the protection may be limited viewing options, parental control, copying restrictions, use restrictions of particular data, where the copy restrictions may be a limited time of copying, such as copying still frames, no copying, copying with copyright notices, and/or reduced quality copying. The central processing unit **12**, upon receipt of the particular level of protection, ensures that the computer system **10** would handle the video data as indicated by the level of protection.

As a further function of the central processing unit **12**, it may determine that the exact type of protection required cannot be processed by the CPU due to user requirements and/or service provider requirements such as generic data access, new licensing provisions, protection levels changes, new hardware which requires a higher level protection, and/or new revision levels. As such, the central processing unit may determine an alternate data access parameter based on at least one of user requirements and service provider requirements. For example, if the CPU received an indication of protection **24** that allows for still frame copying, but newly revised copy restrictions limited such copying, the CPU could default to a no-copying restriction. As one skilled in the art will readily appreciate, the alternate protection may be done in an almost endless variety of ways based on changes to the user and/or service provider requirements.

FIG. **2** illustrates a graphical representation of a field of video data **30**. As is known in the art, video data is presented in a plurality of fields which are displayed at a given rate upon a television set. One such rate is 59.94 hertz, which is commonly used for North American television. Thus, the field of video data **30** is one particular field that would be displayed for approximately 1/60th of a second. The field of video data **30** includes vertical sync and blanking **34** and **36**, horizontal sync and blanking **38** and **40**, and video data for display **32**. If the video data is to be encoded, the horizontal sync lines **38** and **40** and/or the vertical sync lines **36** and **34** would include the embedded data access parameters. For example, the vertical sync lines **34** and **36** may include embedded information that allows close caption to be employed on a television set. The vertical sync lines **34** and **36**—also referred to as vertical blank intervals—may further store information that is referred to as teletext lines, which allow for additional information to be carried in the vertical sync lines **34** and **36**, or Intercast™ lines which allow HTML documents to be embedded in the vertical sync lines **34** and **36**, without disrupting the video data for display **32**. The vertical sync lines **34** and **36** may also include the Macrovision embedded coding.

FIG. **3** illustrates a representation of a horizontal sync line **38** or **40** that includes data access parameters **42**, **44**; screen ends **46**,.**48**; a color burst wave form **50**, and video data for display **52**. As shown, the data access parameters **42** and **44** are embedded in the wave form to indicate that the data being transmitted is to be copy protected. In addition, the color burst wave form **50**, which is shown as a sinusoid, may have a 180 degree phase-shift to further provide an indication of copy protection. The video data **52** contains the actual video that is displayed. The screen ends **46** and **48** indicate the edge of the horizontal line **38** or **40**. Note that the data access parameters **42** and **44** are shown as peaks which are similar to the peaks incorporated in the Macrovision technique. These data access parameters **42** and **44**, however, may further include data access restrictions related to viewing options, parental control, and use restrictions of the particular data.

FIG. **4** illustrates a schematic block diagram of a computer system **60** that includes the video decoder **16**, the central processing unit **12**, the memory **14**, a television encoder **62**, a graphics display **64**, a hard disk **66**, and a monitor **68**. The video decoder **16** is shown to include the graphics controller **20** and the video digitizer **22**. The graphics controller **20** is further shown to include an analog to digital (A/D) converter **70** and a protection detection circuit **72**. In essence, the A/D converter **70** converts the video data stream **18** into a digital signal while the protection detection circuit **72** looks for the data access parameter peaks **42** and **44**. Upon detecting these peaks, the protection detect circuit **72** provides the indication of protection **24** to the CPU **12**.

As an alternative embodiment of the video decoder **16**, the analog to digital converter **70** maybe deleted and the output of the video digitizer **22**, which typically functions as an analog to digital converter, would provide the digital signals to the protection detect circuit **72**. In this configuration, the protection detect circuit **72** would look for the data access parameters **42** and **44** in the digital data and subsequently provide the indication of protection **24**.

The digital video data **26** is provided to memory **14** and to the graphics display **64**. In the embodiment shown, if the video data **18** is provided by a DVD player, the digital data stored in memory **14** does not included the Macrovision encoding, thus, when the memory provides the digital video data **26** to the television encoder **62**, the television encoder **62**, if not informed by the central processing unit of the Macrovision encoding, would process the digital video data **26** without such coding. As mentioned, when the video signal does not include the protection coding, it can be readily copied. Thus, the present invention, via the graphics controller **20**, provides an indication that the central processing unit **12** which, in turn, notifies the television encoder **62** that the data is to be encoded. The television encoder **62**, based on signals from the CPU, activate an encoding process such that the resulting television signals include the protection information. For example, the television encoder **62** could encode the video data with the Macrovision technique.

FIG. **5** illustrates a logic diagram that may be used by the circuits of FIGS. **1** and **4** to detect whether a video and/or audio data stream includes data access protection parameters. The process begins at step **80** where data is received as audio data and/or video data. The process then proceeds to step **82** where a determination is made as to whether the data includes a data access parameter and whether the data access parameter is active. The data access parameter may indicate that the data has particular restrictions such as parental control, viewing options, copy restrictions and/or use restrictions. If the data access parameter is not active, the process proceeds to step **84** where no restrictions regarding use and/or copying are imposed on the data.

If, however, the data access parameter is active, the process proceeds to step **86** where an indication of protection regarding the data is provided. Such an indication is provided to the computer system such that the CPU and affiliated, peripheral devices, or computer elements, are prevented from copying and/or utilizing the data in an unauthorized manner.

FIG. **6** illustrates a logic diagram that may be used to detect the presence of copy protection within a video data stream. The process begins at step **90** where a video data stream is received. Having received the data stream, the process proceeds to step **92** where a determination is made as to whether the video data stream includes copy protection information. If not, the process proceeds to step **94** where no restrictions are imposed on the copying and/or use of the data. If, however, the video data includes copy protection information, such as Macrovision, the process proceeds to